> Is it possible that healthcare organizations will wind up spending more
> money and time meeting HIPAA regulations than they did on the year 2000
> issue? If so, how, and why?
> For at least 50 percent of healthcare organizations, the time and money
> spent by 2003 on making their applications and processes HIPAA-compliant
> will equal or exceed that spent on year 2000 compliance (0.7 probability).
>
>
> Is HIPAA of concern to you and your agency? Gartner has a team of
> analysts who are dedicated to HIPAA and its effect on IT spending and
> government agencies.
>
> <<HIPAA COMPARE.DOC>> <<Alternative Approaches for HIPAA Transaction
> Compliance.pdf>> <<It Is Time for Common Sense.pdf>>
>
>
Please feel free to contact me if you have any questions or concerns.

> Laura Downing
> Public Sector
> Account Manager
> Ph: 888-443-8693 Ext: 4522
> Fa: 941-561-4242
> Laura.Downing@Gartner.com
>
> Gartner
>   Insight for the Connected World
>
>

GartnerGroup

Research Note
Decision Framework
27 July 2000

HIPAA COMPARE Level I: Awareness

Matthew Duncan

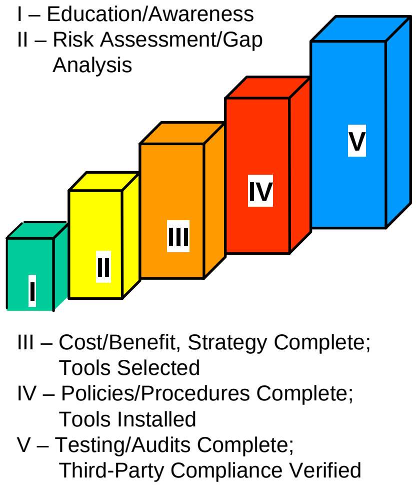
Gartner's COMPARE scale for HIPAA Administrative Simplification defines five levels for tracking compliance activity and readiness. We describe milestones for achieving Level I: Awareness.

Core Topic
Healthcare IT Drivers and Strategies ~ Industry Applications

Key Issue
How will changes in regulatory, societal or technological arenas alter the importance or position of healthcare IT and the IS department?

Gartner introduces its methodology to rate an HCO's activity and readiness for HIPAA Administrative Simplification (AS) mandates, adopting and modifying our COMPARE (see Figure1) scale approach (see Note 1 and *Research Note* COM-11-2070). This methodology will provide HCOs a guideline for moving through HIPAA compliance tasks, and help them avoid being sidetracked by the hype surrounding the regulations.

Figure 1
HIPAA COMPARE Scale


I – Education/Awareness
II – Risk Assessment/Gap Analysis
I
II
III
IV
V
III – Cost/Benefit, Strategy Complete; Tools Selected
IV – Policies/Procedures Complete; Tools Installed
V – Testing/Audits Complete; Third-Party Compliance Verified

Source: Gartner

Note 1
COMPARE for HIPAA
Gartner first copyrighted the COMPARE (COMpliance Progress And REadiness) scale in 1997, as a tool for tracking an enterprise's progress with Year 2000 compliance. This tool, modified for HIPAA AS, will provide the framework for our tracking and reporting of the healthcare industry's overall progress. We will survey

HCOs in all segments on a quarterly basis during the next three years, to deliver a benchmark for an HCO to compare its progress toward HIPAA compliance.

Level I (Awareness) Defined. At the end of this stage, an HCO has completed its organizationwide general education and awareness program, and all preliminary activities are complete. A senior-level individual has been appointed to oversee compliance efforts, and a HIPAA committee or project team has been staffed. These specific milestones are not necessarily sequential, but most HCOs will complete them all before beginning Level II (Assessment) activities.

HIPAA compliance manager appointed. Some HCOs have left HIPAA AS compliance with the same office responsible for compliance with the other HIPAA subtitles (e.g., Risk Management). Others have selected either their former Year 2000 coordinator or a high-level IS manager responsible for security. HIPAA AS is an enormous undertaking, and the majority of HCOs will require a dedicated resource for oversight.

Focused education/awareness training for senior executives complete. Surveys indicate that apathy and lack of understanding abounds, especially in CDOs. Management must understand the risks and opportunities inherent in HIPAA, and realize that AS is a business issue, not just an IS issue.

Executive sponsor appointed. The education process should lead to one executive (see Note 2) being designated to take overall responsibility for complying with HIPAA and exploiting its business advantages (see *Research Note* COM-10-9487). This executive will provide the liaison between the compliance team and an HCO's board and other executives. The sponsor role should be an additional responsibility for an existing executive, since this person must be active in the day-to-day HCO operations to have the clout to effectively intervene on behalf of HIPAA efforts when needed.

Note 2
Sponsor Candidates

A CFO would draw attention to the true reason for AS — to cut administrative waste and save money. A chief operating officer may also be a good option, considering the AS impact on all operations (as well as the need to improve efficiency and develop a culture of fanaticism around patient privacy). Appointment of the CIO is not recommended for sponsorship, since this may lead to the perception of HIPAA AS as "just another IS headache."

HIPAA compliance committee established and staffed. Representatives from human resources, medical records, billing, IS and risk management should form the core of this committee, with oversight from the executive sponsor and compliance manager.

General education/awareness training for all employees complete. HIPPA's transaction and code set standards will have a significant impact on the business processes of most HCO departments. More importantly, the entire enterprise must become fanatical about protecting patient privacy. The communication of these changes and their reasons must begin early.

First round special education of all employed and affiliated physicians complete. The work patterns of doctors will be disturbed as an HCO establishes and enforces the policies required for HIPAA compliance. Physician leaders must be consulted during the process. A first round of awareness is necessary so that they will give the assessment process sufficient attention (see Note 3).

Note 3
Physicians and Privacy

Most doctors believe in protecting patient privacy, but many do not practice sound techniques (e.g., giving receptionists their passwords to retrieve test results, sending patient data in unencrypted e-mails, discussing cases in elevators). They must receive special training to truly embrace the urgency of security and privacy regulations.

Legal counsel contacted and HIPAA expertise assessed. The main objective in Level I is to identify counsel that is closely monitoring HIPAA and its legal ramifications.
AS regulations and implementation guides reviewed by compliance manager and committee. Before beginning compliance assessment efforts, HCOs must understand what they are facing. This is the first step.

Acronym Key

CDO	Care delivery organization
HCO	Healthcare organization
HIPAA	Health Insurance Portability and Accountability Act

Bottom Line: The AS transaction and code set standards will be final by September 2000, and a privacy and security final rule is expected by year-end 2000. Most Level I milestones, however, are not dependent on final rule publication. Most HCOs that have not reached COMPARE Level I compliance before the beginning of 2001 will require crash programs for compliance, with consequentially higher costs. In their resultant haste to meet deadlines, they will also likely sacrifice the benefits of the opportunistic HIPAA requirements around standardized transactions and the use of Internet technologies.

This document has been published by:

Service	**Date**	**Document #**
Healthcare Executive and Management Strategies	27 July 2000	DF-11-5714
PRISM for Healthcare Providers	27 July 2000	DF-11-5714
PRISM for Healthcare Payers	27 July 2000	DF-11-5714

The information contained herein has been obtained from sources believed to be reliable. Gartner Group disclaims all warranties as to the accuracy, completeness or adequacy of such information. Gartner Group shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

Strategic Planning, SPA-12-5910
J. Young

Research Note
9 January 2001

Alternative Approaches for HIPAA Transaction Compliance

Health plans can achieve HIPAA compliance through either a tactical or strategic approach. We discuss business, implementation and ROI implications of each approach.

Core Topic
Industry Applications: Managed Care

Key Issue
How will managed care organizations leverage IT to respond to new competition and changing roles in a consumer-centric environment?

Strategic Planning Assumption
Payers that have not adopted a strategic approach to HIPAA transaction compliance and begun implementation by 2005 will either fail or be acquired by 2008 (0.7 probability).

Note 1
Cautionary Note: The Clearinghouse Solution
Gartner's initial assessment of HIPAA transaction requirements indicates that even a tactical solution relying on a mapping/clearinghouse strategy will require modifications to the back-end processing environment. It will not be possible to comply with HIPAA simply through a clearinghouse solution. A health plan's ability to adequately leverage clearinghouse mapping technologies to achieve HIPAA compliance will depend upon the robustness of the mapping tool, as well as the health plan's back-end core processing and database applications and technologies and current data environment. Health plans expecting to support HIPAA transactions solely through clearinghouse and integration engine technologies are advised to closely evaluate this approach against the established HIPAA standards.

There are two approaches to HIPAA transaction compliance — tactical and strategic. The approach taken will be dictated by corporate business strategy, available resources and technologies. Each approach provides different ROI opportunities, but with vastly different investment requirements (see *Research Note* TU-12-4880).

The Tactical Approach: The tactical approach focuses on the simplest and most cost-effective (in the short term) route to HIPAA transaction compliance. Compliance is viewed as a largely technology problem; the solution includes a heavy reliance on translation and auditing tools, employing internal or outsourced clearinghouse mapping technologies (see Note 1). With this approach, few changes to the back-end processing environment or data model are planned. Health plans will achieve compliance with limited investment and in the context of the existing technological and business environment. Although ROI results will be tangible, they are short-term only and provide few long-term opportunities. Why?

1) As all healthcare organizations must comply with these standards, there is no specific competitive advantage or opportunities gained, other than a (very) short-term edge, if achieved ahead of competitors (see Note 2).

2) The clearinghouse or mapping compliance strategy does nothing to address existing processing inefficiencies and costs, which include:

- *Dumping to Paper:* Many health plans are unable to efficiently input electronic information (particularly enrollment and referrals) and have to print electronically submitted records for (at least some) manual entry. Having the ability to accept electronic HIPAA compliant transactions, without back-end integration, is of limited value, although presumably appealing to external constituents due to the

Note 2
Current Healthcare Payer Data Models and Business Implications
Current healthcare payer data models have inconsistent or multiple references and data elements among, or even within, various applications, creating duplicate record challenges and significant mapping and coding requirements, historically for reporting and, more recently, for Internet initiatives. For example, provider references and ID numbers vary; claim and payment codes vary — particularly for local codes and unique contract terms; and field length and field requirements vary among various applications used to support managed care processing. Data models among and, sometimes, within applications are different and management of the related elements (required fields, field audits, etc.) also vary.

Business implications are many. Health plans have spent millions in both technology and personnel costs managing the impact of poor and unaligned data models — from incorrectly paid claims and rework due to multiple provider numbers and variable-coding schemes for payment, to significant underutilization of data mart and data warehouse initiatives due to poor data, with inconsistent coding and data element use. As health plans are further compelled to share data externally to the enterprise through Internet initiatives, the data management issue becomes that much more significant. Data cleanup efforts are at the core of a strong Internet strategy. HIPAA transaction standards will not address all the data issues, but provide a universal standard from which to start.

Incorporating the HIPAA data standards will eliminate some of these challenges, create a more-consistent data environment, begin to standardize processing logic and so facilitate autoadjudication, and create more-consistent and robust data sources to support customer service and Internet initiatives. Healthcare payers moving to a common standard can also begin to incorporate additional information that is currently available, but frequently discarded in the mapping process, including patient satisfaction, health status and beneficiary information for Medicaid patients.

Note 3
New Business Opportunities
New business opportunities afforded by consistent, reliable and data-rich environments include: more-focused and effective care management services, personalized benefit and healthcare services (positioning for defined contributions) and evolution to a healthcare infomediary (supporting member healthcare financial and clinical decisions).

lower cost of submission. However, constituents that submit electronically will soon expect more-timely responses. Poor back-end integration and requisite manual integration will limit the health plan’s ability to provide the expected and timely responses. Only the front-end process will become more efficient with a tactical approach; the rest of the process will remain inefficient.

- *Poor Internal Data Models:* Even if health plans are able, through a tactical approach, to achieve 100 percent translation and automated entry into back-end systems, overall back-end processing will not be improved, due to continued use of existing (generally poor) data models (see Note 3). Front-end efficiencies are gained but, again, the back-end processing and data environments are unimproved.
- *Continuing Translation or Clearinghouse Vendor Costs:* One of the cost savings opportunities of the HIPAA transaction format standardization is limiting reliance (and therefore licensing or per transaction costs) of translation and clearinghouse technologies through better alignment of transaction data models and a reduction of specialized formats.

Tactical compliance makes existing front-end business processes more efficient by moving to a greater electronic capture environment, but fundamentally only provides incremental improvements to an existing business model.

The Strategic Approach: The strategic approach focuses on improved data models and business processes that will better position the health plan to both reap the administrative benefits *and* to position HIPAA investments as the catalyst to better healthcare outcomes and new business opportunities. This strategy will 1) embrace solutions that integrate new data standards within the core data models of the healthcare payers’ IT applications; and 2) include business process re-engineering to capitalize and promote new business opportunities and better health outcomes (through both business process changes and alignment of other IT initiatives).

Benefits of this approach are:

- The greater the ability to accept HIPAA data elements directly into the back-end environment without translation, the more consistent and reliable the internal data model will be. A more-consistent internal data model ultimately will enable quicker adjudication, customer response, better reporting and improved successes with Internet initiatives.

Note 4
HIPAA Transactions and External Data Sharing
Easier and more-effective data sharing and integration with external sources will only be achieved when all users adopt the HIPAA transaction datasets, rather than mapping strategies. This benefit will evolve incrementally as changes to the data model evolve and also requires adoption of service-oriented architectures to facilitate information sharing. In the meantime, it offers the opportunity for a much richer and more easily managed internal data environment that will place the health plan in a good position for data-sharing opportunities as they evolve.

- The greater the ability to accept HIPAA data elements into the back-end environment reduces translation requirements, minimizing or eliminating translation and clearinghouse technology costs and resource commitment.
- Available data and information is used, rather than discarded as not fitting into proprietary data models, creating richer internal data stores.
- Potentially, data from external sources can be more easily integrated (without the need for extensive translation and formatting), creating better opportunities for a richer overall data environment and new business opportunities (see Note 4).

HIPAA standards are a strong catalyst for an evolution to a new and better business model focused on more-flexible and customer-focused products and services and better health outcomes *if* healthcare payers execute a strategic approach to HIPAA compliance as the basis for creation of a timely and standardized data environment. Enterprises that wish to leverage the promise of electronic connectivity and the Internet as a tool to improve healthcare outcomes must first establish the underlying data model and data integrity to support a shared information environment. Administrative and clinical data sources must come together to finally provide the data-rich and connected environment to improve allocation of healthcare resources and outcomes. Healthcare payers that make strategic data management a principal component of their HIPAA compliance approach will benefit from better data sources from which to guide corporate business decisions and to identify new opportunities.

In addition, it is the new business opportunities that will engender future success. The combination of HIPAA, the Internet, more-robust back-end processing systems and workflow technologies, will create the environment for real-time processing by 2005 (see *Research Note* SPA-10-9948*).* Future health plan differentiation is *not* based on transaction management, but on data management and the delivery of electronic information and services both within the enterprise and with external customers. Healthcare payers must quickly move to leverage the benefits of the data standards set by HIPAA for both short-term benefits and long-term survival.

Moving From a Tactical to a Strategic Approach — An Incremental Approach to a Large Hurdle

In the long term, health plans that do not adopt a strategic approach will not survive. The hard reality, however, is that, in the short term, costs associated with a strategic approach are significant enough to threaten health plan viability. A healthcare payer may understand the benefits of rethinking core data models and business processes, yet plan to use tactical compliance as a means to meet HIPAA deadlines due to resource, business and time limitations. Indeed, such an approach may be necessary in some cases. The approach allows the deferral of process re-engineering until the industry has had some experience with the rollout of transactions, and adoption rates and understands the implications on core technologies and business processes.

In this context, a tactical solution may be a reasonable *short-term* solution particularly for health plans with multiple legacy environments (see Note 5). However, health plans that do not view tactical compliance as just the starting point, and plan to move beyond this to a more strategic approach, will not survive in the long term. Payers that have not adopted a strategic approach to HIPAA transaction compliance and begun implementation by 2005 will fail or be acquired by 2008 (0.7 probability).

Bottom Line: The fundamental issue is whether health plans view HIPAA as a means to improve the existing business (largely a transaction manager) or as an opportunity to move beyond transaction management to a new and better business model and value proposition for the healthcare value chain. Although a tactical approach may be initially required due to technology, business and cost limitations, health plans must not view this as the endpoint. Health plans that differentiate themselves for future success through new business opportunities will create a strategy to embrace HIPAA standards as part of the core data structure and plan for business process redesign around efficiencies created.

Note 5
Core Vendor HIPAA Initiatives
Core managed care vendors are currently assessing their own HIPAA compliance strategies. Several are planning to support much of the HIPAA transaction requirements by enhancing the current data model. Adoption of these vendors' HIPAA-compliant release provides a good opportunity to move toward strategic compliance.

Acronym Key

HIPAA	Health Insurance Portability and Accountability Act
ROI	Return on investment

COM-10-9487
W. Rishel

Research Note
27 April 2000

Commentary

HIPAA: It Is Time for Common Sense

Consultants and vendors are battering HCO executives with their old favorites — fear, uncertainly and doubt. We suggest clear opportunities to prioritize investments and avoid "paralysis by worst-case scenario."

After the immutable deadline for year 2000 passed, the healthcare industry turned its attention to Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification. Attention has grown since the U.S. Department of Health and Human Services (DHHS) recently promised a firm delivery date of its first final rule, on electronic data interchange (EDI) transactions, of June 2000. Allowing for a little more slippage within the U.S. Office of Management and Budget, we predict that DHHS will publish the final rule on HIPAA e-transaction standards in 3Q00, resulting in a compliance date in 4Q02 (0.9 probability). Other than privacy, we believe the other standards will become operational during 2003.

Until recently, there has been management disinterest in HIPAA based on the realities of the federal Balanced Budget Act and the general success in dealing with year 2000. Consultants, vendors and internal HIPAA coordinators have attempted to break through that resistance by listing the substantial civil and criminal penalties in various proposed rules and worst-case interpretations of the regulations' impact on legacy systems. Alarmist tactics have initial value in awakening upper management, but they must quickly be replaced by more measured analysis, lest the healthcare organization (HCO) direct resources to law firms rather than remediation, or overspend and create internal turmoil by attempting to do too much at once.

It Is *Not* Like Year 2000. Analysts, including Gartner, have compared HIPAA to year 2000 as a gross measure of impact and a way to grab attention. It is important, however, not to slavishly follow the metaphor. Unlike year 2000, the deadlines are not fixed and business decisions can be made to delay or minimize conformance with some of the provisions in the early years. Furthermore, many of the requirements are subject to remediation through external, add-on applications, rather than a year-2000-like rework of legacy systems.

It *Is* About Money. HCOs should not be misled by the emphasis on security and privacy; HIPAA is about forcing HCOs to do what other industries did on their own: reduce costs by replacing people, paper and postage with electronic communications. Healthcare costs have risen to 15 percent of the gross domestic product and represent a burden on U.S. firms selling goods abroad. With various programs, including the Balanced Budget Act, the government has played a game of brinksmanship with healthcare, squeezing clinical costs until HCOs start to fail and then backing off slightly. In provider and payer enterprises together, three to four people handle the paper to administer a case for each person who gives hands-on care. Nonetheless, the industry has responded to cost reductions by squeezing clinicians rather than finding ways to streamline the paperwork.

The government sees two opportunities to force the industry to pursue administrative savings through the HIPAA standards:

- Mandating standard e-transactions, codes and identifiers.
- Establishing standards that enable the use of the Internet in lieu of expensive private networks.

In 1994, the Workshop on Electronic Data Interchange built a case that e-transactions could save $73 billion year, or about one-third of all healthcare administrative costs. Both political parties share the view that a substantial portion of these savings can be realized and will generate reductions in the federal budget and improvements in the competitiveness of U.S. firms. HIPAA Administrative Simplification is about the money, and it will not go away.

Creating Change in a Capital-Poor Industry. It takes money to make money or, for that matter, to save money. The investment to comply with HIPAA has a front-loaded component that must be made before the savings are realized. Fully realizing the savings requires considerably more investment than that required for simple compliance. Estimates vary on the cost, but even using the low government estimates, it will take years to realize a return on the investment. After years of cost cutting, providers have razor-thin or nonexistent capital budgets, and payers also face limitations.

The HIPAA security and privacy standards do not themselves directly contribute to the return on investment. They are included to assure the public that there will not be a loss of confidentiality caused by using more EDI. It might have been nice if compliance on these were delayed, so that the industry could begin to use the savings from electronic data exchange to fund compliance. But, of course, this is not legally or politically possible.

Recognizing When "Just Enough" Is Best. While it is not possible to delay compliance with the security and privacy standards, it *is* possible to avoid being frightened by worst-case analyses and committing funds to crash projects. Judicious application of the "80-20" rule can allow an HCO to address the most important concerns first and get to the final details in the outlying years. The proposed rules have made it clear that DHHS intends to ramp up enforcement gradually. The rule on transactions says so explicitly. The proposed Privacy Rule, which is the most challenging, has the weakest enforcement provisions. The secretary of DHHS will accept complaints through an as-yet-unbudgeted office and evaluate them for civil and criminal penalties after attempting to reconcile the parties.

It is clear that the government will initially focus on the most egregious complaints as it and the industry gain experience with the rules and appropriate compliance measures. Accrediting agencies such as the Joint Commission on the Accreditation of Healthcare Organizations have stated an intent to include some of the HIPAA regulations in their certification standards, but integration into their programs will also take time.

For the first year of enforcement for each HIPAA rule, the government will be tentative, focusing on the most egregious and deliberate violators rather than on detailed, across-the-board compliance (0.9 probability). In the second and third years after HIPAA compliance becomes mandatory for each rule, government enforcement, and scrutiny by accrediting agencies, will ramp up gradually, but HCOs that are diligently attempting to meet the standards, and doing as well as the industry in general, will not face severe sanctions (0.8 probability).

During the ramp-up period, as the government and the industry build experience, enforcement priority decisions must be based, in part, on a comparison of the HCO being examined with the industry as a whole. If the HCO did not wantonly ignore a standard for its commercial gain, if it has addressed the most critical issues necessary to comply with a standard and if it is as far along in its compliance as the majority of its peers, it is unlikely to face the dire penalties that the acts describe. In other words, an HCO will be "graded on the curve" in the security and privacy standards, at least for several years.

It is important to keep a realistic view of the enforcement processes in mind when being presented with alarmist analyses of these standards. For example, the alarmist view could lead to a conclusion that all systems must be replaced to precisely establish the "need to know" on every data element, that two-factor public key infrastructure (PKI) based user authentication must be installed everywhere, or that there is a need for some other budget-killing remediation effort. When resources are tight, and priority decisions must be made, the best amount to invest in security and privacy is just enough to meet the most pressing needs immediately and to accompany this with a budget for improving practices over time, as industry compliance improves.

A Common Sense Approach. HCOs should not wait for the final rules. They should begin now to assess their enterprises and identify programs for HIPAA compliance. It is important to assess all the HIPAA requirements together, because the different standards have impact on the same systems, facilities and organizational units. However, in analyzing their response to the assessment, HCOs should consider the requirements in two categories:

- *Opportunistic requirements* are those that provide a return on investment (cost savings). These include the standards that require or enable e-commerce, that is, the transaction, code and national identifier standards. Management should put its most creative and aggressive efforts here, not to simply meet the requirements but to do so in a way that actually captures the cost savings by restructuring in-house processes to take advantage of EDI and the availability of standards. These include streamlining and automating eligibility and referral checking, providing better customer relationship management through online interfaces and automating some collection steps.
- *Support requirements* are necessary and require investment, but do not have the same potential for cost savings. The goal here should be to find the "just enough" level that meets the real needs and keeps the HCO on a par with industry, then to continuously improve compliance over the years.

Bottom Line: It is important to regard HIPAA as an opportunity. A sure path to loss of competitive standing is to find the least-cost methods of compliance with the opportunistic HIPAA requirements without finding a way to capture the cost savings. At the same time, it is not critical to address all requirements maximally. An HCO can defer one-time compliance costs by gauging its response to security and privacy standards to find the threshold of measures that represents responsible, real-world compliance at a level comparable to other HCOs in the industry.